Deeltentamen I, Ringen en Galoistheorie.

16-4-2009, 9-12 uur

Geef een goede onderbouwing van je antwoorden. Succes!

1. (a) (10 pt) Ontbindt het polynoom X^3-3X+3 in irreducibele factoren in $\mathbb{Q}[X]$ en in $(\mathbb{Z}/5\mathbb{Z})[X]$.
   (b) (5 pt) Zij p een priemgetal. Bewijs dat $X^4+p^3X^2+p^5$ irreducibel in $\mathbb{Q}[X]$ is (hint: vervang X door pX).

2. Zij R een ring met 1. Een *idempotent* van R is een element $e \in R$ zó dat $e^2 = e$. Een idempotent heet *triviaal* als $e = 0$ of 1.
   (a) (5 pt) Zij R_1, R_2 een tweetal ringen met 1. Laat zien dat $R = R_1 \times R_2$ een niet-triviale idempotent bevat.
   (b) (10 pt) Zij nu R een ring met 1 en e een idempotent.
      i. Laat zien dat $1 - e$ een idempotent is.
      ii. Laat zien dat $R \cong R/(e) \times R/(1-e)$.

3. Beschouw de ring $\mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} | a, b \in \mathbb{Z}\}$.
   (a) (10 pt) Laat zien dat $2, 3, \sqrt{-6}$ irreducibele elementen in $\mathbb{Z}[\sqrt{-6}]$ zijn.
   (b) (5 pt) Laat zien dat $\mathbb{Z}[\sqrt{-6}]$ geen ontbindigsring is.

4. Beschouw de ring
$$\mathbb{Q}_5 = \left\{ \frac{n}{m} \in \mathbb{Q},\ m \not\equiv 0 (\text{mod } 5) \right\}.$$
   (a) (8 pt) Laat zien dat $\mathbb{Q}_5$ een deelring van $\mathbb{Q}$ is.
   (b) (8 pt) Zij (5) het ideaal in $\mathbb{Q}_5$ voortgebracht door 5. Laat zien dat (5) een priemideaal is.
   (c) (8 pt) Laat zien: $x \in \mathbb{Q}_5^* \iff x \notin (5)$.
   (d) (8 pt) Laat zien dat (5) het enige maximale ideaal in $\mathbb{Q}_5$ is.

5. Zij R een ring met 1 en R' een deelring die 1 bevat.

   (a) (8 pt) Laat zien: $I \subset R$ ideaal $\Rightarrow I \cap R'$ is een ideaal in R'.

   (b) (8 pt) Laat zien: $I \subset R$ priemideaal $\Rightarrow I \cap R'$ is een priemideaal in R'.

   (c) (7 pt) Laat met een voorbeeld zien dat *niet* altijd geldt: $I \subset R$ is maximaal ideaal $\Rightarrow I \cap R'$ is maximaal ideaal in R'.

UITWERKINGEN

1. (a) Het polynoom $X^3 - 3X + 3$ is irreducibel in $\mathbb{Q}[X]$. Dat kunnen we op twee manieren zien.

      i. $X^3 - 3X + 3$ is een monisch Eisenstein polynoom voor $p = 3$. Dus irreducibel.

      ii. Als $X^3 - 3X + 3$ reducibel is, dan moet er een lineaire factor zijn. Bovendien is er een ontbinding in $\mathbb{Z}[X]$ (Gauss' Lemma). Deze moet dus van de vorm $(X - a)(X^2 + bX + c)$ zijn met $a, b, c \in \mathbb{Z}$. Maw a is een geheel nulpunt zijn en een deler van 3. Testen van de delers $\pm 1, \pm 3$ geeft dat geen van allen een nulpunt zijn. Dus is $X^3 - 3X + 3$ irreducibel in $\mathbb{Q}[X]$.

   Als het polynoom $X^3 - 3X + 3$ reducibel in $(\mathbb{Z}/5\mathbb{Z})[X]$ is, dan moet er een nulpunt in $\mathbb{Z}/5\mathbb{Z}$ zijn. Testen van $0, 1, 2, 3, 4$ geeft dat 4 en 2 nulpunten in $\mathbb{Z}/5\mathbb{Z}$ zijn. Ontbinden geeft $X^3 - 3X + 3 \equiv (X - 4)^2(X - 2) \pmod 5$.

   (b) Vervang X door pX. We krijgen een nieuw polynoom $p^4X^4 + p^5X^2 + p^5 = p^4(X^4 + pX^2 + p)$. Het polynoom $X^4 + pX^2 + p$ is irreducibel in $\mathbb{Q}[X]$ precies dan als het oorspronkelijke polynoom $X^4 + p^3X^2 + p^5$ dat is. Merk op dat $X^4 + pX^2 + p$ een Eisenstein-polynoom is voor de priem p en dus irreducibel.

2. (a) Merk op dat $(0,1)$ en $(1,0) \in R_1 \times R_2$ idempotent zijn.

   (b) i. Zij e idempotent. Er geldt: $(1-e)^2 = 1-2e+e^2 = 1-2e+e = 1-e$, dus $1-e$ is idempotent.

   ii. Merk op dat $e + (1-e) = 1$. Dus $1 \in (e) + (1-e)$ waaruit volgt $R = (e) + (1-e)$, maw de hoofdidealen (e) en $(1-e)$ zijn relatief priem. We kunnen nu de Chinese reststelling toepassen,

$$R/(e)(1-e) \cong R/(e) \times R/(1-e).$$

   Merk nu op dat $(e)(1-e) = (e-e^2) = (0)$. Verder geldt voor iedere ring $R/(0) \cong R$, omdat (0) de kern van de identieke afbeelding $R \to R$ is. Conclusie: $R \cong R/(e) \times R/(1-e)$.

3. Bkijk de normafbeelding $N(a + b\sqrt{-6}) = a^2 + 6b^2$. We weten dat $N(\alpha) = \pm 1 \iff \alpha \in \mathbb{Z}[\sqrt{-6}]^*$. Verder zijn er geen elementen met norm 2 of 3. Uit de vergelijking $a^2 + 6b^2 = 2$ zien we namelijk dat $|a| \leq \sqrt{2}$, en dus $a = \pm 1$, en $|b| \leq \sqrt{2/6}$, en dus $b = 0$. Blijft over de elementen ± 1 en deze hebben geen norm 2. Op dezelfde maniet laten we zien dat er geen norm 3 elementen zijn.

   (a) Stel dat $2 = \alpha\beta$ waarin $\alpha, \beta \in \mathbb{Z}[\sqrt{-6}]$ geen eenheden zijn, dwz $N(\alpha), N(\beta) > 1$. Uit de multiplicatieve eigenschap van de norm volgt $4 = N(\alpha)N(\beta)$. Samen met $N(\alpha), N(\beta) > 1$ geeft dit $N(\alpha) = N(\beta) = 2$ en we hebben gezien dat dergelijke elementen niet bestaan. Op dezelfde manier tonen we irreducibiliteit aan van $3, \sqrt{-6}$.

   Een wat onhandiger manier is te proberen $2 = (a + b\sqrt{-6})(c + d\sqrt{-6})$ op te lossen. Uitwerking geeft $2 = ac - 6bd + (ad+bc)\sqrt{-6}$. En dus $2 = ac - 6bd$, $ad + bc = 0$. Vermenigvuldig de eerste met d en pas $ad = -bc$ toe. We krijgen: $2d = -bc^2 - 6bd^2 = -b(c^2+6d^2)$. Met andere woorden, $c^2 + 6d^2$ is een deler van $2d$. Dus $c^2 + 6d^2 \leq 2|d|$. Dat kan natuurlijk alleen maar als $d = 0$. De vergelijkingen worden nu $2 = ac, bc = 0$. Hieruit volgt $b = 0$ en $ac = 2$. De ontbindingen zijn dus $2 \cdot 1, (-2) \cdot (-1)$.

   Er zijn natuurlijk talloze andere manieren om de vergelijkingen op te lossen maar, zoals gezegd, de norm werkt handiger.

   (b) We hebben de ontbindingen $-6 = (\sqrt{-6})^2 = -2 \cdot 3$. Omdat -2 niet $\pm\sqrt{-6}$ is (geen geassocieerde van $\sqrt{-6}$ staan hier twee verschillende ontbindingen van -6 in irreducibele elementen.

4. Beschouw de ring

$$\mathbb{Q}_5 = \left\{ \frac{n}{m} \in \mathbb{Q},\ m \not\equiv 0 (\text{mod } 5) \right\}.$$

(a) Om te laten zien dat $\mathbb{Q}_5$ deelring van $\mathbb{Q}$ is moeten we laten zien dat

i. $\alpha, \beta \in \mathbb{Q}_5 \Rightarrow \alpha - \beta \in \mathbb{Q}_5$.

ii. $\alpha, \beta \in \mathbb{Q}_5 \Rightarrow \alpha \cdot \beta \in \mathbb{Q}_5$.

Stel $\alpha = m/n, \beta = m'/n'$ met n, n' gehele getallen niet deelbaar door 5. Dan zijn

$$\frac{m}{n} - \frac{m'}{n'} = \frac{mn' - m'n}{nn'}, \qquad \frac{m}{n} \cdot \frac{m'}{n'} = \frac{mn}{m'n'}$$

breuken met een noemer die niet deelbaar is door 5. Ze zitten dus in $\mathbb{Q}_5$.

(b) Het ideaal (5) bestaat uit elementen van de vorm m/n waarin m deelbaar is door 5 en n niet. Stel $\frac{a}{b}\frac{a'}{b'} \in (5)$ waarin b, b' niet deelbaar zijn door 5. Dan moet de teller van $\frac{aa'}{bb'}$ deelbaar zijn door 5. Dus 5 deelt a of a'. En dus $\frac{a}{b} \in (5)$ of $\frac{a'}{b'} \in (5)$. Het ideaal (5) is dus een priemideaal.

(c) Stel $m/n \in \mathbb{Q}_5$ en neem aan dat m, n relatief priem zijn. Dan geldt dat $m/n \in \mathbb{Q}_5^* \iff n/m \in \mathbb{Q}_5 \iff 5$ deelt niet $m \iff m/n \notin (5)$.

(d) Zij M een maximaal ideaal. Stel dat M een element x bevat dat niet bevat is in (5). Dan is x een eenheid volgens het voorgaande en volgt uit $x \in M$ dat $M = \mathbb{Q}_5$. Tegenspraak. We concluderen dat $M \subset (5)$ en daarmee is (5) het unieke maximale ideaal.

5. Zij R een ring met 1 en R' een deelring die 1 bevat. Zij I een ideaal.

   (a) Om te laten zien dat $I \cap R'$ een ideaal is moeten we aantonen dat

      i. $0 \in I \cap R'$. Dit klopt omdat per definitie $0 \in I$ en $0 \in R'$.

      ii. $a, b \in I \cap R' \Rightarrow a - b \in I \cap R'$. Dit klopt omdat per definitie geldt $a, b \in I \Rightarrow a - b \in I$ en $a, b \in R' \Rightarrow a - b \in R'$.

      iii. $r \in R', a \in I \Rightarrow ra \in I \cap R'$. Dit klopt ook omdat $a, r \in R' \Rightarrow ra \in R'$ en $r \in R' \subset R, a \in I \Rightarrow ra \in I$.

   (b) Stel $a, b \in R'$ en $ab \in I \cap R'$. Omdat I een priemideaal in R is geldt dat $a \in I$ of $b \in I$. Stel dat het eerste het geval is. Omdat tevens $a \in R'$ geldt nu dat $a \in I \cap R'$.

   (c) In $\mathbb{Q}$ is (0) een maximaal ideaal. In de deelring $\mathbb{Z}$ is het ideaal (0) geen maximaal ideaal.